INRIA

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 1087

Programme 1
Programmation, Calcul Symbolique
et Intelligence Artificielle

CONSTRUCTION OF HILBERT CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS AND DIHEDRAL EQUATIONS MODULO p

François MORAIN

Septembre 1989

RR-1087

CONSTRUCTION OF HILBERT CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS AND DIHEDRAL EQUATIONS MODULO p

Francois MORAIN * †

morain@inria.inria.fr

Abstract. The implementation of the Atkin-Goldwasser-Kilian primality testing algorithm requires the construction of the Hilbert class field of an imaginary quadratic field. We describe the computation of a defining equation for this field in terms of Weber's *class invariants*. The polynomial we obtain, noted $\mathcal{W}(X)$, has a solvable Galois group. When this group is dihedral, we show how to express the roots of this polynomial in terms of radicals. We then use these expressions to solve the equation $\mathcal{W}(X) \equiv 0 \bmod p$, where p is a prime.

CONSTRUCTION DU CORPS DE CLASSE DE HILBERT D'UN CORPS QUADRATIQUE IMAGINAIRE ET EQUATIONS DIHEDRALES MODULO p

Résumé. L'implantation du test de primalité dû à Atkin, Goldwasser et Kilian necessite la construction du corps de classe de Hilbert d'un corps quadratique imaginaire. Nous décrivons le calcul d'un polynôme de définition de ce corps à l'aide des *invariants de classe* de Weber. Le polynôme ainsi obtenu, noté $\mathcal{W}(X)$, a un groupe de Galois résoluble. Quand ce groupe est dihédral, nous montrons comment on peut exprimer les racines de ce polynôme sous forme de radicaux. Nous montrons enfin comment ces expressions permettent le calcul des racines de $\mathcal{W}(X) \equiv 0 \bmod p$ pour p un nombre premier.

---

* Projet ALGO, Institut National de Recherche en Informatique et en Automatique, Domaine de Voluceau, B. P. 105, 78153 LE CHESNAY CEDEX (France) & Département de Mathématique, Université Claude Bernard, 69622 Villeurbanne CEDEX

† On leave from the French Department of Defense, Délégation Générale pour l'Armement.

1 Introduction

One of the problems arising when implementing the so-called Atkin-Goldwasser-Kilian algorithm [23] is the computation of defining equations for the Hilbert class field K_H of an imaginary quadratic field K. The straigthforward approach to this problem yields integer polynomials with very large coefficients. Although this is not a crucial part of the algorithm, it is interesting to have as small coefficients as possible.

In this report, we describe an efficient way of computing the defining polynomial of K_H, called *Hilbert polynomial*. The roots of this polynomial modulo a suitable prime p are exactly the j-invariants of elliptic curves modulo p having complex multiplication by the ring of integers of K[12].

We then explain how it is possible to find elements of K_H whose minimum polynomial (over Q) has smaller coefficients: This is done using Weber's functions. Then, we show how to factor all these polynomials over the genus field of K. We also explain how to solve these equations by radicals and use the resulting expressions to get a root of these polynomials modulo p.

2 Some properties of quadratic forms and fields

Our aim is to recall basic properties of quadratic forms and fields that are necessary for the following sections. We introduce first quadratic forms that are easy to compute with and then quadratic fields that are well suited for explaining the theory. These are two sides of the same object.

2.1 Quadratic forms

The following results are well known and can be found in [13, 10]. Let $-D$ be a fundamental discriminant, i.e. D is a positive integer which is not divisible by any square of an odd prime and which satisfies $D \equiv 3 \bmod 4$ or $D \equiv 4, 8 \bmod 16$. We can factor $-D$ as $q_1^* \cdots q_t^*$, where $q^* = (-1)^{(q-1)/2} q$ if q is an odd prime and -4 or ± 8 otherwise. In the sequel, the q_i's are supposed to be ordered as follows: if $D \equiv 0 \bmod 4$, then $q_1 = 4$ or 8. Then the q's with $q^* = q$ are listed in increasing order and finally the q's with $q^* = -q$, also in increasing order. We put $l = \#\{i, q_i^* = q_i\}$. It is easy to see that

$$t - l - 1 \equiv 0 \bmod 2. \tag{1}$$

A *quadratic form* of discriminant $-D$ is a 3-uple of integers (a, b, c) such that $b^2 - 4ac = -D$. There is a correspondance between the set of quadratic forms and the set of 2×2 matrices with rational coefficients. With $Q = (a, b, c)$, we associate the 2×2 matrix

$$M(Q) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Two forms Q and Q' of same discriminant are said to be *equivalent* (or $Q \sim Q'$) if there exists a N in $SL_2(\mathbf{Z})$ (ie. an integer matrix with determinant ± 1) such that:

$$M(Q') = N^{-1} Q N.$$

This clearly defines an equivalence relation on quadratic forms. It can be shown that:

Proposition 2.1 *Each equivalence class contains exactly one form (a, b, c) with a, b, c relatively prime and satisfying $|b| \leq a \leq c$ and $|b| = a \Rightarrow b > 0$. Such a form is called* reduced.

There is an algorithm that computes a reduced form equivalent to a given form: we refer to the litterature for this.

The set of primitive reduced quadratic forms of discriminant $-D$, noted $\mathcal{H}(-D)$, is finite (for $|b| \leq \sqrt{D/3}$ if (a,b,c) is reduced). Moreover, it is possible to define a law on classes that gives to $\mathcal{H}(-D)$ the structure of a group. This law is called the *composition of classes* and is ordinarily noted multiplicatively. For the actual computation of the law, we refer to [26]. The order of $\mathcal{H}(-D)$ is noted $h(-D)$. The neutral element is called the *principal form* and equals $(1,0,D/4)$ or $(1,1,(D+1)/4)$ according to D mod 4.

Let $C=(a,b,c)$ be an element of $\mathcal{H}(-D)$. For (x,y) in $\mathbf{Z}^2$, put $C(x,y)=ax^2+bxy+cy^2$. Let p be a rational prime. The equation $p=C(x,y)$ has a solution in (x,y) if the following conditions are satisfied:

$$\left(\frac{-D}{p}\right)=+1, \text{ and } \forall i, 1<i\leq t, \left(\frac{p}{q_i}\right)=\left(\frac{a}{q_i}\right). \tag{2}$$

(*Hint:* $4ap=(2ax+by)^2+Dy^2$). Put $\chi_i(a)=\chi_i(C)=\left(\frac{a}{q_i}\right)$ for $i>1$ and $\chi_1(a)=\left(\frac{-D}{p}\right)\prod_{i>1}\chi_i(a)$. This defines a map from $\mathcal{H}(-D)$ to $Z_t=\{\pm 1\}^t$ by:

$$\begin{array}{rccc} \Xi: & \mathcal{H}(-D) & \rightarrow & Z_t \\ & C & \mapsto & (\chi_1(C),\ldots,\chi_t(C)). \end{array} \tag{3}$$

The following theorem was proven by Gauss:

Theorem 2.1 *The map Ξ is onto: If we start from $\varepsilon=(\epsilon_1,\ldots,\epsilon_t)$ satisfying $\prod_i \epsilon_i=+1$, we can find a C such that $\Xi(C)=\varepsilon$. Moreover, let $G_0=\Xi^{-1}(+1,\ldots,+1)$. Then G_0 is non empty and is a subgroup of $\mathcal{H}(-D)$, called the* principal genus. *Its order is $e=h/g$ where $g=2^{t-1}$. We can decompose $\mathcal{H}(-D)$ into classes w.r.t to G_0: $\mathcal{H}(-D)=G_0\cup G_1\cup\cdots\cup G_{t-1}$, with $G_i=C_iG_0$ for a well chosen C_i in $\mathcal{H}(-D)$. The G_i's are called* genera.

2.2 Quadratic fields

Consider now $\mathbf{K}=\mathbf{Q}(\sqrt{-D})$. The extension $\mathbf{K}|\mathbf{Q}$ is abelian of degree 2, of Galois group $\{1,\tau\}$, where τ is the complex conjugation. The ring of integers of $\mathbf{K}$ is $\mathcal{O}_K=\mathbf{Z}[\omega]$, where

$$\omega=\begin{cases} \sqrt{-D/4} \text{ if } D\equiv 0 \bmod 4 \\ \frac{1+\sqrt{-D}}{2} \text{ otherwise.} \end{cases}$$

The conjugate of an element $\alpha=x+y\omega$ is $\alpha'=\tau(\alpha)=x+y\tau(\omega)$. The trace (resp. the norm) of α is $T_K(\alpha)=\alpha+\tau(\alpha)$ (resp. $N_K(\alpha)=\alpha\tau(\alpha)$).

The decomposition of the ideal (p) in $\mathbf{K}$ is given by the following theorem:

Proposition 2.2 *If $(-D/p)=+1$, the ideal (p) splits as the product of two distinct ideals in $\mathbf{K}$. If $(-D/p)=0$, (p) ramifies, and if $(-D/p)=-1$, it is inert.*

We end this section by:

Proposition 2.3 *The equation $p=\pi\pi'$ has a solution in $\mathcal{O}_K$ if and only if (p) splits as the product of two principal ideals in $\mathbf{K}$. This is equivalent to saying that p is represented by the principal form of discriminant $-D$.*

2.3 Genus field

The genus field of $\mathbf{K}$ is $\mathbf{K_G}=\mathbf{Q}(\sqrt{q_1^*},\ldots,\sqrt{q_t^*})$, the q_i being described above. The field $\mathbf{K_G}$ is the maximal abelian extension of $\mathbf{Q}$ above $\mathbf{K}$. The Galois group of $\mathbf{K_G}|\mathbf{Q}$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^t$.

3 Hilbert polynomials

3.1 Weber's functions

We first introduce some functions. Let z be any complex number and put $q = \exp(2i\pi z)$. Dedekind's η function is defined by [28, §24 p. 85]

$$\eta(z) = \eta(q) = q^{1/24} \prod_{m \geq 1} (1 - q^m). \tag{4}$$

We can expand η as [28, §34 p. 112]

$$\eta(q) = q^{1/24} \left(1 + \sum_{n \geq 1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2}) \right). \tag{5}$$

The Weber's functions are [28, §34 p. 114]

$$f(z) = e^{-i\pi/24} \frac{\eta(\frac{z+1}{2})}{\eta(z)}, \tag{6}$$

$$f_1(z) = \frac{\eta(\frac{z}{2})}{\eta(z)}, \tag{7}$$

$$f_2(z) = \sqrt{2}\, \frac{\eta(2z)}{\eta(z)}, \tag{8}$$

$$\gamma_2 = \frac{f^{24} - 16}{f^8}. \tag{9}$$

The *modular invariant* j is defined as [28, §54 p. 179]:

$$j(z) = \frac{(f^{24} - 16)^3}{f^{24}} = \frac{(f_1^{24} + 16)^3}{f_1^{24}} = \frac{(f_2^{24} + 16)^3}{f_2^{24}} = \gamma_2^3. \tag{10}$$

The q-expansion of j is (Cf. [25]):

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n\, q^n, \tag{11}$$

where the c_n's are positive integers. For a survey of their properties, see for instance [23].

3.2 Class field

Let $-D$ be a fundamental discriminant and $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$. The *Hilbert Class Field* of $\mathbf{K}$ is the maximal unramified abelian extention of $\mathbf{K}$ and is noted $\mathbf{K}_\mathrm{H}$[12]. We have (see [6, 28]):

Theorem 3.1 *The field $\mathrm{K_H}$ can be obtained by adjoining to $\mathbf{K}$ any value $j_r = j(\omega_r)$, where $\omega_r = \omega(C_r) = (-b_r + i\sqrt{D})/(2a_r)$ with $C_r = (a_r,\ b_r,\ c_r)$ in $\mathcal{H}(-D)$. The minimum polynomial of the j_r's is noted $H_D(X)$.*

The Galois group of $\mathrm{K_H}|\mathbf{K}$, noted Γ, is isomorphic to $\mathcal{H}(-D)$. If C is an element of $\mathcal{H}(-D)$, the corresponding element σ_C of Γ acts on $j(C')$ by:

$$\sigma_C(j(C')) = j(C^{-1} \cdot C'). \tag{12}$$

Another important property is (see [11])

Proposition 3.1 *A rational prime p splits as $\pi\pi'$ in $\mathbf{K}$ if and only if p splits completely in $\mathbf{K}_H$.*

Several authors ([4, 16, 27]) have listed the values of j for all known values of D of class number 2 or 3, and for some other values. This could be used to compute the corresponding $H_D(X)$. However, this method cannot be applied to polynomials of higher degree and so we must look for a method that always works. The simplest way to do this is the following (see [20, 11, 21]): Compute some floating point approximation to j_r with sufficiently many digits and then form $\prod_{r=1}^{h}(X - j_r)$.

We need a way to check our computations. This is done as follows. It is possible to compute $\mathcal{N} := H_D(0)$ independently as the norm of j_r in $\mathbf{Q}(j)$, using a theorem of Gross and Zagier: Let z be a quadratic number satisfying $Az^2 + Bz + C = 0$. Define $\mathrm{disc}(z) = B^2 - 4AC$. Then:

Theorem 3.2 ([17, 14]) *Let $-D_1$ and $-D_2$ be two different fundamental discriminants. We put:*

$$J(D_1, D_2) = \left(\prod_{\substack{[z_1],\,[z_2] \\ \mathrm{disc}(z_i) = D_i}} (j(z_1) - j(z_2)) \right)^{4/(w_1 w_2)} \tag{13}$$

where the product is extended to all reduced forms of discriminants $-D_1$ and $-D_2$, and w_i is the number of units in $\mathbf{Q}(\sqrt{-D_i})$. If l is a prime number satisfying $(D_1 D_2/l) \neq -1$, we introduce:

$$\epsilon(l) = \begin{cases} (D_1/l) & \text{if } (l, D_1) = 1 \\ (D_2/l) & \text{if } (l, D_2) = 1. \end{cases} \tag{14}$$

If $n = \prod l_i^{\alpha_i}$ with $(D_1 D_2/l_i) \neq -1$ for all i, we extend ϵ by $\epsilon(n) = \prod \epsilon(l_i)^{\alpha_i}$. Then:

$$J(D_1, D_2)^2 = \pm \prod_{\substack{x^2 < D_1 D_2 \\ x^2 \equiv D_1 D_2 \bmod 4}} F\left(\frac{D_1 D_2 - x^2}{4} \right) \tag{15}$$

where

$$F(m) = \prod_{\substack{nn' = m \\ n, n' > 0}} n^{\epsilon(n')}. \tag{16}$$

As a particular case

Corollary 3.1

$$J(D, -3)^2 = (\mathcal{N})^{\frac{2}{3}}. \tag{17}$$

This formula shows that $\mathcal{N}^{\frac{2}{3}}$ and therefore $\mathcal{N}$ are always rational integers.

We now give some details of the actual computation.

3.3 Numerical evaluation of $j(z)$

We want to evaluate $j(z)$ as fast as possible. Atkin suggests two ways of doing it. The first one is to compute in sequence $\eta(z)$, $\eta(2z)$, $f_2(z)$ and $j(z)$. The second is to use the following proposition:

Proposition 3.2 ([28, §72 p. 253]) *If*

$$x = 5\left(\frac{\eta(5z)}{\eta(z)}\right)^2,$$

then:

$$\gamma_2(z) = x^5 + 10x^2 + \frac{5}{x}. \tag{18}$$

We use the first approach.

3.3.1 Choice of the parameters

Let us define:

$$\mathcal{N}(q) = \sum_{n\geq 1}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2}),$$

and

$$\mathcal{N}_N(q) = \sum_{n=1}^{N}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2}).$$

We want to compute the error made when computing $\mathcal{N}_N(q)$ instead of $\mathcal{N}(q)$. We put $q = \rho\exp(i\theta)$ and we replace $\exp(i\alpha)$ by its trigonometric expansion. We introduce two functions $\mathcal{C}$ (resp. $\mathcal{C}_N$) and $\mathcal{S}$ (resp. $\mathcal{S}_N$) corresponding to the real and imaginary parts of $\mathcal{N}$ (resp. $\mathcal{N}_N$).

Let $\mathcal{E}(q) = \mathcal{C}(\rho) - \mathcal{C}(q)$ (resp. $\mathcal{E}_N(q) = \mathcal{C}_N(\rho) - \mathcal{C}_N(q)$). Then:

$$\mathcal{E}(q) = \sum_{n\geq 1}(-1)^n\left(\rho^{n(3n-1)/2}(1-\cos(n(3n-1)/2)) + \rho^{n(3n+1)/2}(1-\cos(n(3n+1)/2))\right).$$

This is an alternating series with positive real coefficients and we deduce

$$|\mathcal{E}(q) - \mathcal{E}_N(q)| \leq 2\,(\rho^{(N+1)(3N+2)/2} + \rho^{(N+1)(3N+4)/2}) = 2e_{N+1}.$$

Now, we can come back to the problem of estimating

$$\begin{aligned}\mathcal{C}(q) - \mathcal{C}_N(q) = &\ (\mathcal{C}(q) - \mathcal{C}(\rho)) + (\mathcal{C}_N(\rho) - \mathcal{C}_N(q)) + (\mathcal{C}(\rho) - \mathcal{C}_N(\rho)) \\ = &\ (\mathcal{E}_N(q) - \mathcal{E}(q)) + (\mathcal{C}(\rho) - \mathcal{C}_N(\rho)).\end{aligned}$$

Hence:

$$|\mathcal{C}(q) - \mathcal{C}_N(q)| \leq 3e_{N+1}.$$

Coming back to $\mathcal{N}$, we see that:

$$|\mathcal{N}(q) - \mathcal{N}_N(q)| \leq 6e_{N+1}.$$

Looking at $e_n = \rho^{n(3n-1)/2}(1+\rho^n)$, it is not hard to see that $e_n \leq \rho^{3(n-1)^2/2}$ as soon as $\rho < 1/4$ and $n \geq 5$. We have proved:

Proposition 3.3

$$|\mathcal{N}(q) - \mathcal{N}_N(q)| \leq 6\rho^{3N^2/2}. \tag{19}$$

We have to evaluate j for values of z of the form $z = (-b+i\sqrt{D})/2a$, where $(a,\ b,\ (b^2+D)/4a)$ is a primitive reduced form of discriminant $-D$. We put $q = \rho e^{i\theta}$, with $\rho = e^{-\pi\sqrt{D}/a}$ and $\theta = -\pi\, b/a$. Since this form is reduced: $a \leq \sqrt{D/3}$. We deduce: $\rho \leq e^{-\pi\sqrt{3}} < 4.34 \times 10^{-3}$.

3.4 Computation of $H_D(X)$

First, we group the forms according to their genus. Inside each genus, we make two classes of forms. In the first one, we put all forms (a,b,c) for which $(a,-b,c)$ is also reduced. The second gathers the remaining forms. This is motivated by the fact that the values of j corresponding to the forms (a,b,c) and $(a,-b,c)$ are conjugate (in $\mathbf{C}$). After we have computed the h values of j, we build $H_D(X)$.

Using the q-expansion of j, it is not hard to see that $\log|j| \approx \pi\sqrt{D}/a$. The number of digits of $j(q)$ is asymptotically $\pi\sqrt{D}/(a\log 10)$. We have to compute the coefficients of $H_D(X)$ to within 0.5 and in particular the product $\prod j_r$. The precision required is thus:

$$\mathrm{Prec}(D) = \frac{\pi\sqrt{D}}{\log 10}\sum\frac{1}{a} + \nu_0, \tag{20}$$

where the sum is taken over all primitive reduced forms of discriminant $-D$, and ν_0 a positive constant that takes care of the error made in our estimation of $\log|j|$ (typically $\nu_0 = 10$).

Suppose we want to compute $j(a,b)$. Then, using (3.3), we compute $\eta(kz)$ to the order:

$$\sqrt{S \times \frac{a}{k}}, \tag{21}$$

where:

$$S = \frac{2}{3}\,\frac{\log 6 + \mathrm{Prec}(D)\log 10}{\pi\sqrt{D}}. \tag{22}$$

We then form all products of the form $X - j$, grouping terms of the type $(X-j)$ and $(X-\bar{j})$ to get:

$$(X-j)(X-\bar{j}) = X^2 - (j+\bar{j})X + j\bar{j},$$

which reduces error computations.

We check the result with (17). If we find that $H_D(0)$ is the cube of an integer to within 0.5, we are confident that the computed polynomial is indeed the one we were looking for.

The coefficients of these polynomials are huge. For example, we compute:

$$H_{23}(X) = X^3 + 3491750X^2 - 5151296875X + 12771880859375.$$

4 Weber polynomials

Let $u(z)$ denote any modular function: Weber calls $u(\omega)$ a *class invariant* if $u(\omega)$ is in $\mathrm{K}(j(\omega)) = \mathrm{K_H}$ (ω is the generator of $\mathcal{O}_K$). The following results can be found in [28, §125-144] or in [5] or [24].

4.1 The singular invariant γ_2

Theorem 4.1 ([28, §125, p. 459]) *Let z be a quadratic number defined by $Az^2 + Bz + C = 0$. If*

$$3|B, 3\not|A, 3\not|B^2 - 4AC, \tag{23}$$

we have:

$$\mathbf{Q}(\gamma_2(z)) = \mathbf{Q}(j(z)).$$

Starting from a form (a,b,c) of discriminant $-D \not\equiv 0 \bmod 3$, it is always possible to find an equivalent form satisfying the above conditions: Let k be any integer. Then $(A,B,C) = (a, b+2ak, c+bk+ak^2) \sim (a,b,c)$. The algorithm is the following:

procedure GOODC(C)
(* returns a form $C' \sim C$ satisfying (23) *)

1. if $a \not\equiv 0 \bmod 3$, then choose k such that: $B \equiv b + 2ak \equiv 0 \bmod 3$; return $C' = (a, B, c + bk + ak^2)$;
2. if $a \equiv b \equiv 0 \bmod 3$, then surely c is not (since (a,b,c) is primitive); replace (a,b,c) by $(c,-b,a)$ and go to step 1;
3. if $a \equiv 0 \bmod 3$, but $b \not\equiv 0 \bmod 3$, then find k such that $C \equiv c + bk + ak^2 \not\equiv 0 \bmod 3$. Then $(a,B,C) \sim (C,-B,a)$ and we are back to the first case.

The minimum polynomial of γ_2, noted $G_D(X)$, is thus of degree $h(-D)$ and it turns out that its coefficients are smaller than those of the original $H_D(X)$. For example, for $D = 23$, we find:

$$G_{23}(X) = X^3 + 155X^2 + 650X + 23375.$$

4.2 Using other class invariants

We use some power of the functions f, f_1 or f_2. We extract the following results from [21] (alternatively, see the references above). It is assumed from now on that $D \not\equiv 0 \bmod 3$. With each value of D mod 32, we have a canonical choice for u. Hence, we note $W_D(X)$ the corresponding minimal polynomial.

D	u	$W_D(0)$	$\deg(W_D)$
$7 \bmod 8$	$f(\sqrt{-D})/\sqrt{2}$	-1	h
$3 \bmod 8$	$f(\sqrt{-D})$	$(-2)^h$	$3h$
$0 \bmod 4$			
$D/4 \equiv \pm 2 \bmod 8$	$f_1(\sqrt{-D})/\sqrt{2}$	± 1	h
$5 \bmod 8$	$f(\sqrt{-D})^4$	$\pm 2^h$	h
$1 \bmod 8$	$f(\sqrt{-D})^2/\sqrt{2}$	$(-1)^h$	h

Weber also gives conditions for more general z to satisfy the same properties. We now summarize these conditions, as formulated by Atkin. These conditions should be easily deduced from [28, §127, p. 469] (see also [24]).

Theorem 4.2 *Put $D = 4m$ and suppose $Az^2 + 2Bz + C = 0$ with $4B^2 - 4AC = -4m$, A and C odd, $3|B$.*

1. *in the case where $m \equiv 1, 5, \pm 2 \bmod 8$: if $B \equiv 2((2/A) - 1) \bmod 8$, then $f(z)^2/\sqrt{2}$ (resp. $f(z)^4$, $f_1(z)/\sqrt{2}$) is a class invariant;*
2. *in the case where $m \equiv 3, 7 \bmod 8$: if $B \equiv 4((2/A) - 1) \bmod 16$, then $f(z)/\sqrt{2}$ (resp. $f(z)$) is a class invariant;*

We describe below an algorithm (possibly not the best, but this is not a crucial point) for the case $m \equiv 7 \bmod 8$ (the other cases work in the same way). We start from a primitive form (a,b,c) of discriminant $-4m$ and we write $\xi(a) = 4((2/a) - 1)$ when a is odd.

procedure CFOR7(a, b, c)
(* Returns a form $C' \sim (a,b,c)$ satisfying (4.2) *)

1. Make a odd: if a is even then c is odd, since otherwise (a,b,c) would not be primitive. Replace (a,b,c) by $(c,-b,a)$.

2. Make c odd: if c is even then replace (a,b,c) with $(a,b+a,c+b+a)$. (* after this step, a and c are odd and $b=2b'$ *)

3. If $b \equiv 0 \bmod 3$, we are done, since a cannot be divisible by 3, since otherwise, D itself should be congruent to 0 modulo 3. Go to step 6.

4. Make $a \not\equiv 0 \bmod 3$: if $a \equiv 0 \bmod 3$ and $c \not\equiv 0 \bmod 3$, then replace (a,b,c) with $(c,-b,a)$. Otherwise, replace (a,b,c) by $(c+2b+4a,-(b+4a),a)$.

5. Make $b \equiv 0 \bmod 3$: take k even, such that $k \equiv (-b/2)a^{-1} \bmod 3$. Then the required form is $(a,b+2ak,c+bk+ak^2)$.

6. Make $b/2 \equiv \xi(a) \bmod 16$: choose k such that: $b/2+ak \equiv \xi(a) \bmod 16$ and $b/2+ak \equiv 0 \bmod 3$ using the chinese remainder theorem.

4.3 Remarks

A naive approach to the computation of W_D is to use polynomial factorization. Let us see how it works in the case $D=23$. First of all, we substitute $X=(Y-16)^3/Y$ in H_{23} and factor the resulting numerator. We get:

$$(Y^3+22Y^2+853Y-1)$$
$$\times(Y^6-166Y^5+3503765Y^4-412493295Y^3+14351421440Y^2-2785017856Y+68719476736).$$

Now, we substitute $Y=Z^{24}$ in the factor of degree 3 and we factor the result:

$$(Z^3+Z^2-1)(Z^3-Z^2+1)(Z^6+Z^4+2Z^2+1)(Z^{12}-3Z^8+2Z^4+1)$$
$$(Z^6-Z^5+Z^4-2Z^3+Z^2+1)(Z^6+Z^5+Z^4+2Z^3+Z^2+1)$$
$$(Z^{24}+3Z^{20}+7Z^{16}+8Z^{12}+7Z^8-2Z^4+1)(Z^{12}-Z^{10}-Z^8+3Z^4-2Z^2+1)$$

Then W_{23} is the reciprocal polynomial of $-1+Z^2+Z^3$, which is

$$W_{23}(Z)=Z^3-Z-1.$$

It is clear that this method is very expensive, since for the case of class number h, we must factor polynomials with degree $3h$.

Another approach designed by Kaltofen and Yui [21] makes use of the LLL algorithm and is, too, very expensive.

One of the phase of Atkin's test is to factor the polynomials H_D (resp. G_D and W_D) over $\mathbf{Z}/p\mathbf{Z}$. This can be expensive, since the complexity of such computations is basically proportional to the square of the polynomial (see section 6): This explains why we discard the case $D/4 \equiv 3 \bmod 8$, since in this case, we might work on polynomials of degree $3h$.

We shall see in the following section how this computation can be simplified by factoring these equations over the genus field of $\mathbf{K}$. In order to simplify the notation, we will refer to $W_D(X)$ as the defining polynomial of $\mathbf{K}_\mathbf{H}$ corresponding to whichever $H_D(X)$ or $G_D(X)$ or $W_D(X)$ we can use. We call W_D a *Weber polynomial* associated with $-D$.

5 Factoring the equations over the genus field

The aim of this section is to explain how it is possible to factor our $\mathcal{W}_D$'s over $\mathbf{K}_G$. We will show that $\mathcal{W}_D$ has exactly g factors each of degree $e = h/g$ with coefficients in $\mathbf{K}_G$. This reduces the time needed to compute a root of $\mathcal{W}_D$ mod p for large p, since we have to find a root of degree e instead of h.

$$\begin{array}{ll} \mathbf{K}_H & \\ | & e = h/g \\ \mathbf{K}_G & \\ | & g \\ \mathbf{K} & \end{array}$$

We first give some properties of composite quadratic fields, including the computation of an integral basis. Then, we set up an ordering on the genera of $\mathcal{H}(-D)$ through the action of the Galois group of $\mathbf{K}_G|\mathbf{K}$. After proving the preceding results, we detail our algorithm and give some examples.

5.1 Some properties of composite quadratic fields

Let $u_1, \ldots, u_n$ be n distinct non zero elements of $\mathbf{Z}$. We put $k_n = \mathbf{Q}(\sqrt{u_1}, \ldots, \sqrt{u_n})$ and $g = 2^n$. Following [8], we introduce the sequence $\{A_i\}_{0 \le i < g}$ defined by:

$$\begin{aligned} &A_0 = 1, \\ &A_j = \begin{cases} u_{k+1} \text{ if } j = 2^k, \\ A_{2^{k-1}} A_i / \gcd(A_{2^{k-1}}, A_i)^2 \text{ if } j = 2^{k-1} + i \text{ and } 0 < i < 2^{k-1}. \end{cases} \end{aligned}$$

We define also $\alpha_i = \sqrt{A_i}$. Then $\{1, \alpha_1, \ldots, \alpha_{g-1}\}$ is a basis for $k_n|\mathbf{Q}$.

Proposition 5.1 ([8]) *The integers of k_n are necessarily of the form:*

$$x = \frac{1}{2^n} \sum_{i=0}^{g-1} P_i \alpha_i, \tag{24}$$

where the P_i's are rational integers of the same parity, and all even if there is an i in $\{0, \ldots, g-1\}$ such that $A_i \not\equiv 1 \bmod 4$.

5.2 Computations in $\mathbf{K}_G|\mathbf{K}$

The genus field $\mathbf{K}_G = \mathbf{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$ can be described as

$$\mathbf{K}_G = \mathbf{K}(\sqrt{u_1}, \ldots, \sqrt{u_{t-1}}), \tag{25}$$

where

$$u_i = \begin{cases} q_i & \text{for } 1 \le i \le l \\ q_t q_i & \text{for } l < i < t. \end{cases}$$

The Galois group of $\mathbf{K}_G|\mathbf{K}$ is $\Sigma_G = < \varphi_1, \ldots, \varphi_{t-1} >$ where:

$$\varphi_i(\sqrt{u_j}) = \begin{cases} -\sqrt{u_i} & \text{if } j = i, \\ \sqrt{u_j} & \text{if } j \ne i. \end{cases}$$

Hence, Σ_G is isomorphic with $2_{t-1} \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$, and we can represent an element ϕ of Σ_G by a $(t-1)-$ *uple* of *signs* (i.e. elements of $\{\pm 1\}$). We decide to use the following ordering of the ϕ_i. If i is an integer between 0 and $2^{t-1}-1$, we can write: $i = \sum_{s=0}^{t-1} \nu_{s+1} 2^s$ ($\nu_i \in \{0,1\}$) and we take:

$$\phi_i = \varphi_1^{\nu_1} \circ \cdots \circ \varphi_{t-1}^{\nu_{t-1}}.$$

We represent ϕ_i by $(e_1, \ldots, e_{t-1})$ where $e_s = 2\nu_s - 1$.

With this ordering, the i-th conjugate of an integer θ of $\mathbf{K_G}$ is $\theta^{(i)} = \phi_i(\theta)$.

5.3 Ordering the genera

We recall that the Artin symbol associated with the quadratic form C (in fact with the genus G containing C) is (see [9]):

$$\mathcal{A}_G = \left(\frac{\mathbf{K_G}|\mathbf{K}}{\mathfrak{p}}\right) \simeq (\chi_1(G), \ldots, \chi_t(G)),$$

with $\chi_i(G) = (q_i^*/p)$, where $(p) = \mathfrak{p}\mathfrak{p}'$ is any prime number represented by a form of G (Cf. [23]).

We show how to express the ϕ_i's in terms of $\mathcal{A}_G$. Let us write $\phi_i = (e_1, \ldots, e_{t-1})$ and $\mathcal{A}_G = (\epsilon_1, \ldots, \epsilon_t)$. What we have to solve is the system:

$$\left\{\begin{array}{lcl} \epsilon_1 & = & e_1 \\ & \cdots & \\ \epsilon_l & = & e_l \\ \epsilon_{l+1}\epsilon_t & = & e_{l+1} \\ & \cdots & \\ \epsilon_{t-1}\epsilon_t & = & e_{t-1}. \end{array}\right. \tag{26}$$

We compute:

$$\prod_{i=1}^{t-1} e_i = \left(\prod_{i=1}^{t-1} \epsilon_i\right) \epsilon_t^{t-l-1}.$$

With (1), we can simplify:

$$\prod_{i=1}^{t-1} e_i = \prod_{i=1}^{t-1} \epsilon_i = \epsilon_t.$$

The solution of the system (26) is thus

$$\epsilon_i = \left\{\begin{array}{ll} e_i & \text{for } 1 \leq i \leq l, \\ \prod_{i=1}^{t-1} e_i & \text{if } i = t, \\ \epsilon_t e_i & \text{for } l < i < t. \end{array}\right. \tag{27}$$

We take the ordering on the genera to be that induced by the preceding process. Let us give an example. Suppose that $-D = -308 = (-7) \times (-11) \times (-4)$. We take $u_1 = (-1) \times (-7)$ and $u_2 = (-1) \times (-11)$. The ϕ_i's and the associated genera are given below.

i	ϕ_i	G_i
0	$(+,+)$	$(+,+,+)$
1	$(-,+)$	$(+,-,-)$
2	$(+,-)$	$(-,+,-)$
3	$(-,-)$	$(-,-,+)$

(28)

It should be noted that the genus associated with ϕ_0 is always G_0, the principal genus. Moreover the ordering on the ϕ_i's depends only on g and not on D, whereas the correspondance with the genera depends on D and l. With each pair (t, l) satisfying $l \equiv t-1 \bmod 2$, we associate the *generic ordering* defined by the above process. The example given above is the generic ordering $(3, 0)$.

We end this subsection by introducing:

$$J_i = J(G_i) = \{j(C), C \in G_i\} = \{j_{i1}, \ldots, j_{ie}\}, 0 \leq i < g.$$

and

$$\mathcal{W}_D{}^{(i)}(X) = P(J_i) = P(G_i) = \prod_{r=1}^{e}(X - j_{ir}).$$

We remark that $\mathcal{W}_D = \prod \mathcal{W}_D{}^{(i)}$ and that each $\mathcal{W}_D{}^{(i)}$ has only real roots, since two conjugate j's are in the same J.

5.4 The fundamental theorem

We can now state our theorem.

Theorem 5.1 *For all i, $\mathcal{W}_D{}^{(i)}(X)$ is in $\mathrm{K_G}[X]$.*

Proof. For the sake of brevity, we write $\mathcal{W}_i$ for $\mathcal{W}_D{}^{(i)}$. By Galois theory, $\mathrm{K_H}|\mathrm{K_G}$ is normal and we can find an algebraic integer, ζ, of degree e, such that: $\mathrm{K_H} = \mathrm{K_G}(\zeta)$. The conjugates of ζ are $\zeta_1 = \zeta, \ldots, \zeta_e$. We put:

$$\Sigma_H = \mathrm{Gal}(\mathrm{K_H}|\mathrm{K})$$

and

$$\Sigma_{HG} = \mathrm{Gal}(\mathrm{K_H}|\mathrm{K_G}) = \{\psi_1, \ldots, \psi_e\}.$$

Then:

$$\Sigma_H = \Sigma_G \times \Sigma_{HG},$$

that is to say that an element σ of Σ_H can be represented as a pair (ϕ, ψ) where ϕ is in Σ_G and ψ in Σ_{HG}. Following our preceding notations, we decide to write:

$$\Sigma_H = \{\sigma_{ir} = (\phi_i, \psi_r), 0 \leq i < g, 1 \leq r \leq e\}.$$

We have:

Lemma 5.1

$$\forall\, i = 0..g-1, \forall\, r = 1..e, \sigma_{ir}(\mathcal{W}_0) = \mathcal{W}_i. \tag{29}$$

Proof. Remember that:

$$\forall\, i, \forall\, r, \forall\, C, \sigma_{ir}(j(C)) = j(C_{ir}^{-1}C). \tag{30}$$

We know also that $G_i = C_{ir}^{-1}G_0$ for any i, r. The result follows together with (30). ■

We now deal with $\mathcal{W}_0$, containing all the j associated with the principal genus. Let us apply σ_{0r} on $\mathcal{W}_0$. By the preceding lemma, we have:

$$\sigma_{0r}(\mathcal{W}_0) = \mathcal{W}_0.$$

On the other hand:

$$\sigma_{0r}(\mathcal{W}_0) = \sigma_{0r}(\mathcal{W}_0(\zeta)) = \mathcal{W}_0(\psi_r(\zeta)) = \mathcal{W}_0(\zeta_r).$$

Hence, we deduce that all the ψ_r act trivially on the coefficients of $\mathcal{W}_0(X)$ considered as elements of $\mathrm{K_G}(\zeta)$. So $\mathcal{W}_0$ is an element of $\mathrm{K_G}[X]$. With lemma (5.1), we conclude that $\mathcal{W}_i$ satisfies the same property. This ends the proof of our theorem. ■

As a corollary, we have:

Corollary 5.1 *For all i, $\phi_i(\mathcal{W}_0) = \mathcal{W}_i$.*

This motivates our choice of the ordering on the G's, since otherwise we would have to justify that the ϕ's permute the $\mathcal{W}_i$'s.

This result yields an algorithm for computing the expression of $\mathcal{W}_0$ over $\mathrm{K_G}$. We describe this algorithm in the next section.

5.5 Description of the algorithm

The preceding results make it clear that the critical parameters are h and g and not $-D$. Our purpose is now to explain how we can compute the coefficients of $\mathcal{W}_0$ and to exemplify the use of symbolic manipulation in the process.

We are looking for the coefficients of the polynomial $\mathcal{W}_0(X)$ which is a factor of $\mathcal{W}_D$ over $\mathrm{K_G}$. In fact, since the coefficients of $\mathcal{W}_0$ are real, we can work over k_{t-1} defined above. The results are still valid by identifying $\mathrm{K_G}|\mathbf{K}$ to $k_{t-1}|\mathbf{Q}$.

We write:

$$\mathcal{W}_0(X) = X^e + \sum_{r=0}^{e-1} \left(\sum_{s=0}^{g-1} a_{sr}\alpha_s \right) X^r, \tag{31}$$

where all the a_{sr} are in $(1/g)\mathbf{Z}$ and the α_s's as in the preceding section. We will find these coefficients by means of the resolution of a linear system. Let $\alpha_s^{(i)} = \phi_i(\alpha_s)$.

For any polynomial $Q(X)$, let $[X^r]Q$ denote the coefficient of degree r of Q. Then:

$$\sum_{s=0}^{g-1} a_{sr}\alpha_s = [X^r]\mathcal{W}_0. \tag{32}$$

Suppose now that r is fixed, $0 \le r \le e-1$. If we apply $\sigma_{i0} = (\phi_i, 1)$ to (32), we find:

$$\sum_{s=0}^{g-1} a_{sr}\alpha_s^{(i)} = [X^r]\mathcal{W}_i. \tag{33}$$

We do the same thing for $i = 0..g-1$ and we see that $(a_{s,r})_{0\le s<g}$ is the solution of the linear system:

$$\begin{cases} x_0 + x_1\alpha_1^{(0)} + \cdots + x_{g-1}\alpha_{g-1}^{(0)} = Y_0 \\ x_0 + x_1\alpha_1^{(1)} + \cdots + x_{g-1}\alpha_{g-1}^{(1)} = Y_1 \\ \qquad\qquad \cdots \\ x_0 + x_1\alpha_1^{(g-1)} + \cdots + x_{g-1}\alpha_{g-1}^{(g-1)} = Y_{g-1}, \end{cases} \tag{34}$$

where we replace Y_i by $[X^r]\mathcal{W}_i$. We call the preceding system the *generic system of order* g, since it depends only on g. We see that we have just to solve this system once for each different value of g, computing all the a_{sr}'s by replacing the values of the α's by their corresponding floating point approximations.

From a practical point of view, we compute an approximation to $ga_{s,r}$, take the nearest integer and then divide out by the same g. When we have computed our $\mathcal{W}_1$, we compute L, the lcm of the denominators of the coeffcients and we store the coefficients of $L\mathcal{W}_0$.

In the following paragraph, we give some examples.

5.6 Examples

We treat some examples with increasing values of g.

5.6.1 The case $g = 2$

If $g(-D) = 2$, this means that D has only two divisors. Write $-D = q_1(-q_2)$. Then $\alpha_1 = \alpha = \sqrt{u_1} = \sqrt{q_1}$. There is only one generic ordering, namely $(2,1)$:

i	ϕ_i	G_i
0	$(+)$	$(+,+)$
1	$(-)$	$(-,-)$.

The generic system of order 2 is:

$$\begin{cases} x_0 + x_1\alpha &= Y_0 \\ x_0 - x_1\alpha &= Y_1, \end{cases}$$

whose solution is:

$$x_0 = \frac{Y_1 + Y_2}{2}, x_1 = \frac{Y_1 - Y_2}{2\alpha}.$$

Let $-D = -39 = (13)(-3)$. We have $h = 4$ and we classify the four classes of reduced forms into two genera as follows:

$$\begin{aligned} G_0 = G(+,+) &= \{(1,1,10),(3,3,4)\} \\ G_1 = G(-,-) &= \{(2,1,5),(2,-1,5)\} \end{aligned}$$

The corresponding values of j are respectively

$$\begin{aligned} j_{00} &= -331532893.6400821524400563 \\ j_{01} &= -190.2302555961769624634679 \\ j_{10} &= 743.9351688743085105775428 + 18197.25231378441890365623\, i \\ j_{11} &= 743.9351688743085105775428 - 18197.25231378441890365623\, i \end{aligned}$$

The Weber polynomial is $\mathcal{W}_{39} = H_{39}$ and the polynomials $\mathcal{W}_i$ are then:

$$H_{39}^{(0)}(X) = (X - j_{00}) \times (X - j_{01}) = X^2 + 331533083.87033774862X + 63067587095.692979567$$

$$H_{39}^{(1)}(X) = (X - j_{10}) \times (X - j_{11}) = X^2 - 1487.8703377486170212X + 331693431.30702043331.$$

We write $H_{39}^{(0)} = X^2 + (a_{11}\alpha + a_{01})X + (a_{10}\alpha + a_{00})$. We use the solution of the generic system to get:

$$2\begin{pmatrix} a_{11} \\ a_{01} \\ a_{10} \\ a_{00} \end{pmatrix} = \begin{pmatrix} 17399806263 \\ 63399280527 \\ 91951146 \\ 331531596 \end{pmatrix}$$

Hence, we deduce that the two factors of H_{39} over $\mathbf{Q}(\sqrt{13})$ are:

$$2X^2 + (\pm 91951146\alpha + 331531596)X \pm 17399806263\alpha + 63399280527.$$

5.6.2 The case $g = 4$

We have in this case $\theta = \sqrt{u_1} + \sqrt{u_2}$ and the generic system of order 4 is:

$$\left\{ \begin{array}{rcl} x_0 + x_1\alpha_1^{(0)} + x_2\alpha_2^{(0)} + x_3\alpha_3^{(0)} & = & Y_0 \\ x_0 + x_1\alpha_1^{(1)} + x_2\alpha_2^{(1)} + x_3\alpha_3^{(1)} & = & Y_1 \\ x_0 + x_1\alpha_1^{(2)} + x_2\alpha_2^{(2)} + x_3\alpha_3^{(2)} & = & Y_2 \\ x_0 + x_1\alpha_1^{(3)} + x_2\alpha_2^{(3)} + x_3\alpha_3^{(3)} & = & Y_3 \end{array} \right. \tag{35}$$

where:

$$\left\{ \begin{array}{rcl} \alpha_1 & = & \sqrt{u_1} \\ \alpha_2 & = & \sqrt{u_2} \\ \alpha_3 & = & \sqrt{u_1 u_2} \end{array} \right.$$

For $g = 4$, there are two generic orderings, namely $(3,0)$ and $(3,2)$. Let us consider the case where $-D = -308 = (-7) \times (-11) \times (-4)$. The generic ordering is $(3,0)$ and was given in section (5.3).

We want to get the expression of $G_{308}^{(0)}$ over $\mathbf{K}_G$. We have:

$$\begin{array}{rcl} G_{308} & = & X^8 - 95835320X^7 - 923879753200X^6 + 121516780240000X^5 - 195287646706560000X^4 \\ & & -162741620553600000X^3 + 3543368746860800000X^2 + 1361283710251520000000X \\ & & -1293704102704640000000 \end{array}$$

Suppose that we have built the sets of roots of G_{308} according to the genera. We have in this case:

$$\begin{array}{rcl} J_1 = J(+,+,+) & = & \{880456353882407955305050.260304, 797.592915355\} \\ J_2 = J(+,-,-) & = & \{5648.96421088 \pm 8460.8161800511\ i\} \\ J_3 = J(-,+,-) & = & \{3456.226641, -938326357130.70446379\} \\ J_4 = J(-,-,+) & = & \{-47921735.6519096497 \pm 83004169.578235232\ i\}. \end{array}$$

Finally, we obtain:

$$\begin{array}{rcl} G_{308}^{(0)} = & & X^2 + (-23958830 - 9057440\alpha_1 - 7223840\alpha_2 - 2730910\alpha_3)X \\ & & +222228600 + 84022400\alpha_1 + 66972800\alpha_2 + 25321800\alpha_3 \end{array}$$

5.6.3 The case $g = 8$

Let us consider the case $D = 1540$. Since $D/4 \equiv 1 \bmod 8$, we can take as invariant $u = f^2/\sqrt{2}$. A convenient $\mathbf{Q}$-basis is generated by $\{\sqrt{5}, \sqrt{7}, \sqrt{11}\}$. We find that:

$$W_{1540}^{(0)}(X) = 4X + (-59 - 24\alpha_1 - 18\alpha_2 - 7\alpha_3 - 27\alpha_4 - 10\alpha_5 - 8\alpha_6 - 3\alpha_7).$$

5.7 Concluding remarks

We have described above an elegant method of computing the coefficients of $\mathcal{W}_0$. It should be noted that the implementation of this program is rather complex. An easier approach is to compute the coefficients of $\mathcal{W}_0$ by factoring $\mathcal{W}_D$ over $\mathbf{K}_G$ with an appropriate package of multivariate polynomial factorization, such as exists in MACSYMA, REDUCE or MAPLE.

For those interested, I list below a typical example of use of MAPLE [7]. The time needed to factor the polynomial G_{308} is roughly 830s using MAPLE or 970s with MACSYMA on a SUN 3/60 (12 Mo). I implemented the method described above in MAPLE and the computation took only 8s...

```
    |\^/|
._|\|   |/|_. INRIA - Rocquencourt
 \  MAPLE  /  Version 4.2 --- Dec 1987
 <____ ____>  For on-line help, type  help();
      |

# This is G
#          308
> p;

      8            7                6                    5
p := X  - 95835320 X  - 923879753200 X  + 121516780240000 X

                          4                          3                          2
   - 195287646706560000 X  - 1627416205536000000 X  + 35433687468608000000 X

   + 1361283710251520000000 X - 1293704102704640000000

#
# This is the minimum polynomial of alpha=sqrt(7)+sqrt(11)
#
> q;
                                    4       2
                         q := RootOf(_Z  - 36 _Z  + 16)

# Factor p over this field
> evala(Factor(p,q));

                              4       2
(619360 X - 110560 RootOf(_Z  - 36 _Z  + 16) X

                     4       2     2                      4       2      3
 - 1365455 RootOf(_Z  - 36 _Z  + 16)  X + 229200 RootOf(_Z  - 36 _Z  + 16)  X

      2                                4       2
   + X  - 5667600 + 1225600 RootOf(_Z  - 36 _Z  + 16)

                       4       2     2                    4       2      3
   + 12660900 RootOf(_Z  - 36 _Z  + 16)  - 2131200 RootOf(_Z  - 36 _Z  + 16) )

...

Time=      839.1 real       827.2 user         4.5 sys
```

6 Solving $\mathcal{W}_D(X) \equiv 0 \bmod p$

6.1 Girstmair's method †

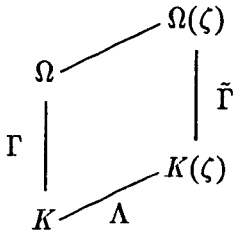
In [15], Girstmair describes an algebraic-numerical method for solving cyclic equations of prime degree over algebraic number fields. We can apply this method to the resolution of our equations $\mathcal{W}_D(X) \bmod p$ in the case where its Galois group is cyclic, which happens whenever $\mathcal{H}(-D)$ is cyclic. This occurs in particular when $h(-D)$ is a prime number.

Suppose that d is a prime number. Let $f(X)$ be a monic irreducible polynomial of degree d in $K[X]$ (K any algebraic number field) whose roots (in $\mathbf{C}$) are $x_1, \ldots, x_d$. Let $\Omega = K(x_1, \ldots, x_d)$ be the splitting field of f and $\Gamma = \mathrm{Gal}(f) = \mathrm{Gal}(\Omega|K)$ the Galois group of f. We suppose from now on that Γ is cyclic, generated by σ and that the x_j's are ordered in such a way that:

$$\sigma x_j = x_{j+1} \text{ if } j < d \text{ and } \sigma x_d = x_1. \tag{36}$$

We make the convention that $x_i = x_j$ whenever $i \equiv j \bmod d$.

Let ζ be a primitive d-th root of unity (e.g. $\zeta = \exp(2i\pi/d)$). We consider the following diagram of extensions:



The extension $\Omega(\zeta)|K(\zeta)$ is abelian, of Galois group $\tilde{\Gamma}$ isomorphic to Γ, since f is supposed irreducible. The corresponding generator of $\tilde{\Gamma}$ is $\tilde{\sigma}$ given by:

$$\tilde{\sigma}(x_j) = \sigma(x_j) \text{ and } \tilde{\sigma}(\zeta) = \zeta. \tag{37}$$

The extension $K(\zeta)|K$ is also abelian and its Galois group is:

$$\Lambda = \{\lambda_1, \ldots, \lambda_d\},$$

where $\lambda_k(\zeta) = \zeta^k$. The *Fourier transform* (in old-fashioned terminology: *Lagrange resolvent*) is defined as an application from $\mathbf{C}^d$ to $\mathbf{C}^d$ acting on $(x_1, \ldots, x_d)$ as

$$F(x_1, \ldots, x_d) = (y_1, \ldots, y_d)$$

where

$$y_k = \sum_{j=1}^{d} x_j \zeta^{-jk}, 1 \leq k \leq d. \tag{38}$$

We can recover the x_j's from the y_k with:

$$x_j = \frac{1}{d} \sum_{k=1}^{d} y_k \zeta^{jk}. \tag{39}$$

---

†Part of this work was done while the author was visiting the University of Illinois at Chicago.

From their definition, we see that the y_k's are algebraic numbers of $\Omega(\zeta)$. The y_k's for $k < d$ cannot be both zero, since otherwise, we would have: $x_1 = \cdots = x_d = y_d/d$. Suppose that $y_1 \neq 0$. Put $z^{(k)} = y_1^{d-k} y_k$, $1 \leq k \leq d$. In particular, we get $y_1^d = z^{(1)}$ and

$$\forall k, y_k = \left(\frac{z^{(k)}}{z^{(1)}}\right) y_1^k. \tag{40}$$

We deduce

$$\forall j, dx_j = z^{(d)} + y_1\zeta^j + \sum_{k=2}^{d-1} \left(\frac{z^{(k)}}{z^{(1)}}\right) (y_1\zeta^j)^k. \tag{41}$$

Solving $f(x) = 0$ is thus reduced to the computation of the $z^{(k)}$'s. We now describe how this computation can be carried out. First of all:

Lemma 6.1 $\forall k, z^{(k)} \in K(\zeta)$.

Proof. We have

$$\begin{aligned}
\tilde{\sigma}(y_k) &= \sum_{j=1}^{d} \tilde{\sigma}(x_j)\tilde{\sigma}(\zeta^{-jk}) && (42)\\
&= \sum x_{(j+1 \bmod d)}\zeta^{-jk} && (43)\\
&= \sum x_j \zeta^{-(j-1)k} && (44)\\
&= \zeta^k y_k. && (45)
\end{aligned}$$

Then:

$$\tilde{\sigma}(z^{(k)}) = \zeta^{d-k}\zeta^k z^{(k)} = z^{(k)}. \blacksquare$$

A basis of $\Omega(\zeta)|K(\zeta)$ is $\{1, \zeta, \ldots, \zeta^{d-1}\}$. We can write: $z^{(k)} = \sum_{j=1}^{d-1} c_j^{(k)} \zeta^{-j}$, where $c_j^{(k)}$ is an element of K. The Galois group of $\Omega(\zeta)|K$ is the direct product of Γ and Λ. The conjugates of $z^{(k)}$ in $\Omega(\zeta)$ are:

$$z_l^{(k)} = \sigma_l(z^{(k)}) = \sum_{j=1}^{d-1} c_j^{(k)} \zeta^{-jl}, 1 \leq l \leq d. \tag{46}$$

On the other hand:

$$z_l^{(k)} = \sigma_l(z^{(k)}) = \sigma_l(y_1^{d-k} y_k) = y_l^{d-k} y_{lk}.$$

Putting $c_d^{(k)} = 0$ and using the Fourier transform, we get

Proposition 6.1 *For all k, $1 \leq k \leq d$, and all j, $1 \leq j \leq d$, we have*

$$dc_j^{(k)} = \sum_{l=1}^{d} z_l^{(k)} \zeta^{jl}, 1 \leq j < d. \tag{47}$$

Moreover $dc_j^{(k)}$ is an integer of K, since it is a combination of algebraic numbers.

We have also: $c_d^{(k)} = 0 = z_1^{(k)} + \cdots + z_d^{(k)}$. If we replace $z_d^{(k)}$ by its values, we find:

Corollary 6.1

$$dc_j^{(k)} = \sum_{l=1}^{d-1} z_l^{(k)} (\zeta^{jl} - 1), 1 \leq j < d. \tag{48}$$

Let $[K : \mathbf{Q}] = m$ and let $\{b_1, \ldots, b_m\}$ be a $\mathbf{Q}$-basis for $K|Q$. Let also $\{\rho_1, \ldots, \rho_m\}$ be all embeddings of $K \to \mathbf{C}$. We have:

$$\forall k, dc_j^{(k)} = c_{j,1}^{(k)} b_1 + \cdots c_{j,m}^{(k)} b_m,$$

with $c_{j,i}^{(k)}$ in $\mathbf{Z}$. We write:

$$\begin{aligned} \forall i, \rho_i(dc_j^{(k)}) &= \textstyle\sum_{r=1}^{m} c_{j,r}^{(k)} \rho_i(b_r) \\ &= \textstyle\sum_{l=1}^{d-1} \rho_i(z_l^{(k)})(\zeta^{jl} - 1). \end{aligned} \tag{49}$$

Then the $c_{j,r}^{(k)}$ can be computed by means of the resolution of $m \times m$ linear systems.

6.2 Application to $\mathbf{K_H}|\mathbf{K}$

Put $K = \mathbf{K} = \mathbf{Q}(\sqrt{-D})$ and $f = \mathcal{W}_D$. Then $\Omega = \mathbf{K_H}$ and $\Gamma = \mathcal{H}(-D)$ is cyclic. With the help of (12), it is possible to properly order the roots of $\mathcal{W}_D(X)$ and apply the preceding results. In particular, we can write:

$$b_1 = \frac{1}{2}, b_2 = \frac{\sqrt{-D}}{2},$$

and $\rho_1 = Id$, $\rho_2 = \tau$ (complex conjugation). In that particular case, it is possible to show:

Lemma 6.2 $\forall j, \forall k, c_{d-j}^{(k)} = \overline{c_j^{(k)}}$.

Thus, we can write:

Corollary 6.2

$$z^{(k)} = \sum_{j=1}^{\frac{d-1}{2}} c_j^{(k)} (\zeta^j + \zeta^{-j}). \tag{50}$$

The algorithm is the following:

procedure FINDC;

1. Compute a floating approximation to y_k;
2. compute the $z_l^{(k)}$ in the same way;
3. find the nearest integer to $dc_j^{(k)}$ using (48);

6.3 Example

Let $D = 47$. Since $D \equiv 7 \bmod 8$, we must study $\mathcal{H}(-4 \times 47) =< (3, 2, 16) >$. Denoting this form by C and putting $u(z) = f(z)/\sqrt{2}$, we find:

$$\begin{aligned} C^2 &= (7, 6, 8) \\ C^3 &= (7, -6, 8) \\ C^4 &= (3, -2, 16) \\ C^5 &= (1, 0, 47) = I \end{aligned}$$

The corresponding u values are

$$\begin{aligned} x_1 &= u(C) &&= -0.16615 + .93871i \\ x_2 &= u(C^2) &&= -0.70119 - .37771i \\ x_3 &= u(C^3) &&= -0.70119 + .37771i \\ x_4 &= u(C^4) &&= -0.16615 - .93871i \\ x_5 &= u(C^5) &&= 1.734691 \end{aligned}$$

so that $\mathcal{W}_{47} = W_{47}(X) = X^5 - X^3 - X^2 - X - 1$. We compute

$$\begin{aligned} y_1 &= 4.108061694 \\ y_2 &= 3.392134996 \\ y_3 &= -.251798809 \\ y_4 &= 1.425046116 \\ y_5 &= 0 \end{aligned}$$

We find for the $z_l^{(k)}$:

$k\backslash l$	1	2	3	4
1	1169.997101	449.1233526	−0.0010122	5.876849839
2	235.171126	55.6222178	−0.0655840	−0.728686003
3	−4.249399	47.2697398	0.0903517	6.888599965
4	5.854177	−0.8541355	−0.8541355	5.854177361

(51)

and for the $2dc_j^{(k)} = [c_{j,1}^{(k)}, c_{j,2}^{(k)}]$:

$k\backslash j$	1	2	3	4
1	[−650, 80]	[−975, 15]	[−975, −15]	[−650, −80]
2	[−105, 15]	[−185, 5]	[−185, −5]	[−105, −15]
3	[−35, 1]	[−15, −3]	[−15, 3]	[−35, −1]
4	[−2, 0]	[−8, 0]	[−8, 0]	[−2, 0]

6.4 Working modulo p

The obvious approach to solving $\mathcal{W}_D(X) \equiv 0 \bmod p$ is to use Berlekamp's algorithm [3, 22]. The complexity of this algorithm is roughly:

$$O((d^3 + d^2(\log p))(\log d)(\log p)^2),$$

if we use standard algorithms. The alternate way is to use what the preceding expressions we described above and work over some finite field $\mathsf{F}(p^e)$ instead of $\mathbf{C}$.

The formula (41) is valid in $\mathbf{Z}/p\mathbf{Z}(\sqrt{-D}, \zeta)$. Since we want to find the roots of $\mathcal{W}_D(X)$ modulo a prime p which splits in $\mathbf{Q}(\sqrt{-D})$, $-D$ is a square in $\mathbf{Z}/p\mathbf{Z}$ and we are to work in $\mathbf{Z}/p\mathbf{Z}(\zeta)$. It is easy to see that d-th roots of unity modulo p live in $\mathsf{F}(p^e)$ where e is the order of p modulo d. This is equivalent to saying that the d-th cyclotomic polynomial $\Phi_d(z)$ splits modulo p as the product of $\phi(d)/e$ factors of degree e, any of which, say $f(z)$, generates $\mathsf{F}(p^e)$ as:

$$\mathsf{F}(p^e) = \mathsf{F}(p)[z]/(f(z)).$$

We can now compute the $z_l^{(k)}$ in $\mathsf{F}(p^e)$, then extract a root of z_1 (for the actual computation, see below). The theory tells us that the resulting formula for x_d will utlimately yield an element of $\mathbf{Z}/p\mathbf{Z}$.

We first introduce our algorithm for extracting roots and then give some numerical examples.

6.4.1 Extracting d-th roots over finite fields

We use an extension of the algorithm of [1] as described in [19, 2] (see also [18]). All computations are supposed to be done modulo $(p, f(z))$. We assume that d divides the order of $\mathsf{F}(p^e)^*$, that is $d|m := p^e - 1$.

function GFPROOT(A, d, p, e, $f(z)$)
(* Extracts a d-th root of A in $\mathsf{F}(p^e) \simeq \mathsf{F}(p)[z]/(f(z))$ *)

1. put $m := p^e - 1$;
2. find a generator of the group of the d-th roots of unity in $\mathsf{F}(p^e)$:
   1. choose B at random in $\mathsf{F}(p^e)$;
   2. $E := B^{m/d}$;
   3. **if** $E^i \neq 1$ for $1 \leq i < d$ **then** E is the generator we were looking for: **go to** (3.); **else go to** (2.1);
3. $e_1 := m/d$; $e_2 := 0$; $d_1 := \gcd(e_1, d)$;
4. **while** $d_1 \neq 1$ **do**
   1. $e_1 := e_1/d_1$; $e_2 := e_2/d$;
   2. **while** $A^{e_1}B^{e_2} \neq 1$ **do** $e_2 := e_2 + m/d_1$;
   3. $d_1 := \gcd(e_1, d)$;
5. compute $g := (-e_1)^{-1} \bmod d$;
6. $X := A^{(ge_1+1)/d}B^{ge_2/d}$ is a root of A in $\mathsf{F}(p^e)$.
7. **end.**

6.4.2 $p \equiv 1 \bmod d$

In that case, we can find a primitive d-th root of unity in $\mathbf{Z}/p\mathbf{Z}$. As an example, let $p = 761$ which splits in $\mathbf{Q}(\sqrt{-47})$ with $761 = 3^2 + 47 \times 4^2$. One of the square roots of -47 is 570. Since $p \equiv 1 \bmod 5$, there are five roots of unity in $\mathbf{Z}/761\mathbf{Z}$. In order to find one, we randomly compute $x^{\frac{761-1}{5}}$ and whenever the result is different from 1, it is a 5-th root of 1. In our case, we take $\zeta = 67 (= 2^{152} \bmod 761)$. Using the algorithm of [29], one finds $y = 547^{1/5} \bmod 761 = 381$ and $x = 590$ is a root of $W_{47} \bmod p$.

6.4.3 $p \equiv -1 \bmod d$

We are looking for a root of $W_{71}(X) = X^7 - 2X^6 - X^5 + X^4 + X^3 + X^2 - X - 1$ modulo $p = 293$. The c matrix is:

$i\backslash j$	1	2	3
1	$[-13829, -2849]$	$[-43152, -3752]$	$[-63690, -1778]$
2	$[-976, -196]$	$[-3621, -263]$	$[-5160, -156]$
3	$[-433, -19]$	$[-764, -60]$	$[-703, -33]$
4	$[-12, 12]$	$[26, 14]$	$[163, 3]$
5	$[-23, -3]$	$[-32, -2]$	$[-70, 0]$
6	$[-4, 0]$	$[-18, 0]$	$[-16, 0]$

We have to solve $2y^7 = (-13829-2849\sqrt{-47})\zeta^6+(-43152-3752\sqrt{-47})\zeta^5+(-63690-1778\sqrt{-47})\zeta^4+(-63690+1778\sqrt{-47})\zeta^3+(-43152+3752\sqrt{-47})\zeta^2+(-13829+2849\sqrt{-47})\zeta$.

We find:

$$\Phi_7(z) = z^6+z^5+z^4+z^3+z^2+z+1 = (z^2+16z+1)(z^2+239z+1)(z^2+39z+1) \bmod 293.$$

and choose $z^2+16z+1$ as a defining polynomial for $\mathsf{F}(p^2)$. We have then to compute a 7-th root of:

$$\begin{aligned} z_1 = {} & 147(235+81R)z^6+147(212+57R)z^5+147(184+273R)z^4 \\ & +147(184+20R)z^3+147(212+236R)z^2+147(235+212R)z, \end{aligned} \tag{52}$$

with $R = \sqrt{-47}$. We take $R \equiv 148 \bmod 293$ in this formula and we get $y^7 = 253z+99 = (78z+193)^7$. Finally $x = 126$ is a root of W_{71} mod 293.

6.4.4 $p \not\equiv \pm 1 \bmod n$

Take for example $p = 1811$, whose order modulo 7 is 6. We take:

$$\mathsf{F}(p^6) = \mathsf{F}(p)[z]/(\Phi_7(z)).$$

We then compute

$$\begin{aligned} y &= 1636z^5+1773z^4+726z^3+1480z^2+1652z+1402 \\ &= (1560z^5+1226z^4+1047z^3+1647z^2+1211z+141)^7 \end{aligned}$$

and find that $x = 1235$ is a root of W_{71} mod 1811.

6.4.5 Extension of the method

It seems plausible that the preceding method applies whenever $\mathcal{H}(-D)$ is a cyclic group, without the restriction h prime. As an example, consider the case $D = 104$ with

$$W_{104}(X) = X^6-2X^5-2X^4+2X^2-2X-1.$$

Then, with the same program, we find that $\mathcal{H}(-104)$ is generated by $(5,4,6)$ and the c matrix is:

$k\backslash j$	1	2	3	4	5
1	$[-8848,156]$	$[-15310,-480]$	$[-12924,0]$	$[-15310,480]$	$[-8848,-156]$
2	$[-356,48]$	$[-962,42]$	$[-1212,0]$	$[-962,-42]$	$[-356,-48]$
3	$[-106,6]$	$[-106,-6]$	$[0,0]$	$[-106,6]$	$[-106,-6]$
4	$[-72,0]$	$[-110,-6]$	$[-76,0]$	$[-110,6]$	$[-72,0]$
5	$[-8,0]$	$[-22,0]$	$[-28,0]$	$[-22,0]$	$[-8,0]$

Take for example $p = 659 = -1 \bmod 6$. We have:

$$\Phi_6(z) = z^2-z+1,$$

which is irreducible in $\mathbf{Z}/659\mathbf{Z}$. We find that $y_1^6 = 402z+266 = (147z+107)^6$ and finally $x = 532$ is a root of W_{104} mod 659.

When $\mathcal{H}(-D)$ is not cyclic, we may do a lot of things. It is possible to do the preceding work over a tower of extensions. When h is even, we can also work directly on $\mathcal{W}_D{}^{(0)}$, when G_0 is cyclic. This implies that we take $K = \mathrm{K_G}$, which is no longer a quadratic field, but a compositum.

7 Conclusions

We have shown how to construct the Hilbert class field of an imaginary quadratic field using Weber's functions. We solved the resulting equations by radicals through factorization over intermediate fields. The final expressions can be used to find the j-invariants of elliptic curves modulo p, where p is a large prime.

Acknowledgments. I'd like to thank O. Atkin for explaining to me some of the subtleties involved in the computation of $\mathcal{W}_D(X)$ and J. Cougnard for answering my questions on composite quadratic fields and for sending me [8].

References

[1] L.M. Adleman, K. Manders, and G. L. Miller. On taking roots in finite fields. In *Proc. 18th Annual IEEE Symp. Foundations of Computer Science*, pages 175–178, 1977.

[2] T. Berger. Résolution de l'équation $X^n = A$ dans un corps fini. Rapport de DEA, Département de Maths, Université de Limoges, Juin 1988.

[3] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. of Comp.*, 24(111):713–735, 1970.

[4] W. E. H. Berwick. Modular invariants expressible in terms of quadratic and cubic irrationalities. *Proc. London Math. Soc.*, 28:53–69, 1928.

[5] B. J. Birch. Weber's class invariants. *Mathematika*, 16:283–294, 1969.

[6] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J. P. Serre. *Seminar on complex multiplication.* Number 21 in Lect. Notes in Math. Springer, 1966.

[7] B. W. Char, K. O. Geddes, G. H. Gonnet, and S. M. Watt. *MAPLE Reference Manual, Fourth Edition.* Symbolic Computation Group, Department of Computer Science, University of Waterloo, 1985.

[8] D. Chatelain. Bases normales de l'anneau des entiers de certaines extensions abéliennes de Q. *Comptes Rendus de l'Académie des Sciences de Paris*, 270:557–560, mars 1970. Ser. A.

[9] H. Cohn. *A classical invitation to algebraic numbers and class fields.* Universitext. Springer-Verlag, 1978.

[10] H. Cohn. *Advanced number theory.* Dover, New York, 1980.

[11] H. Cohn. *Introduction to the construction of class fields.* Number 6 in Cambridge studies in advanced mathematics. Cambridge University Press, 1985.

[12] M. Deuring. Die Klassenkörper der komplexen Multiplikation. In *Enzyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, volume Bd 1, H. 10, T. 2. Teubner, Stuttgart, 1958.

[13] L. E. Dickson. *History of the Theory of Numbers*, volume I, II, III. Chelsea, New York, 1952.

[14] D. R. DORMAN. Special values of the elliptic modular function and factorization formulae. *J. für die Reine und Angew. Math.*, 383:207–220, 1988.

[15] K. GIRSTMAIR. Ueber die praktische Auflösung von Gleichungen höheren Grades. *Mathematische Semesterberichte*, Band XXXIV/1987(Heft 2):213–245, 1987.

[16] A. G. GREENHILL. Table of complex multiplication moduli. *PLMS (1)*, 21, 1891.

[17] B. H. GROSS AND D. B. ZAGIER. On singular moduli. *J. für die Reine und Angew. Math.*, 355:191–220, 1985.

[18] M-D. A. HUANG. Factorization of polynomials overf finite fields and factorization of primes in algebraic number fields. In *Proc. 16th ACM STOC*, pages 175–182, 1984.

[19] M-D. A. HUANG. Riemann hypothesis and finding roots over finite fields. In *Proc. 17th ACM STOC*, pages 121–130, 1985.

[20] E. KALTOFEN AND N. YUI. Explicit construction of the hilbert class fields of imaginary quadratic fields with class numbers 7 and 11. In *Proc. EUROSAM '84*, pages 310–320, Cambridge (England), 1984.

[21] E. KALTOFEN AND N. YUI. Explicit construction of the hilbert class fields of imaginary quadratic fields by integer lattice reduction. Research Report 89-13, Renseelaer Polytechnic Institute, May 1989.

[22] D. E. KNUTH. *The Art of Computer Programming: Seminumerical Algorithms.* Addison-Wesley, 1981.

[23] F. MORAIN. Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm. Rapport de Recherche 911, INRIA, Octobre 1988.

[24] R. SCHERTZ. Die singulären Werte des Weberschen Funktionen f, f_1, f_2, γ_2, γ_3. *J. für die Reine und Angew. Math.*, 286-287:46–74, 1976.

[25] J. P. SERRE. *Cours d'arithmétique.* PUF, 1970.

[26] D. SHANKS. Class number, a theory of factorization, and genera. In *Proc. Symp. Pure Math.*, pages 415–440. AMS, 1971. volume 20.

[27] G. N. WATSON. Ramanujans Vermutung über Zerfällungsanzahlen. *J. für die Reine und Angew. Math.*, 179:97–128, 1938.

[28] H. WEBER. *Lehrbuch der Algebra*, volume I, II, III. Chelsea Publishing Company, New York, 1902.

[29] H. C. WILLIAMS. Some algorithms for solving $x^q \equiv N \bmod p$. In *Proc. 3rd South East Conference on Combinatorics, Graph Theory and Computing*, pages 451–462, 1972.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique